Cryptanalyzing a chaos-based image encryption algorithm using alternate structure

Yu Zhang[a,b], Chengqing Li[c,*], Kwok-Wo Wong[d], Shi Shu[a], Guanrong Chen[d]

[a] *School of Mathematics and Computational Science, Xiangtan University, Xiangtan 411105, Hunan, China*
[b] *MOE (Ministry of Education) Key Laboratory of Intelligent Computing and Information Processing, Xiangtan University, China*
[c] *College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China*
[d] *Department of Electronic Engineering, City University of Hong Kong, Hong Kong*

Abstract

Recently, a chaos-based image encryption algorithm using alternate structure (IEAS) was proposed. This paper focuses on differential cryptanalysis of the algorithm and finds that some properties of IEAS can support a differential attack to recover equivalent secret key with a little small number of known plain-images. Detailed approaches of the cryptanalysis for cryptanalyzing IEAS of the lower round number are presented and the breaking method can be extended to the case of higher round number. Both theoretical analysis and experiment results are provided to support vulnerability of IEAS against differential attack. In addition, some other security defects of IEAS, including insensitivity with respect to changes of plain-images and insufficient size of key space, are also reported.

Keywords: image, chaos, cryptanalysis, differential attack, encryption

1. Introduction

Security of multimedia data including image and video become more and more important as transmission of multimedia data occurs more and more frequently in the current digital world. However, the big differences between multimedia data and text, such as bulk size of multimedia data and strong redundancy existing in neighboring elements of its uncompressed version, make the traditional text encryption algorithms like DES (Data Encryption Standard) can not protect multimedia data efficiently. In addition, multimedia encryption has other special requirements, like fast encryption speed and easy cascade with the whole system. So, designing specific multimedia encryption algorithm become an urgent task. Meanwhile, chaos theory was developed in depth in the 1960s. The most famous character of chaos is so-called "butterfly effect", i.e., states of a chaos system are very sensitive to changes of its initial conditions and control parameters. This character is very similar to the confusion and diffusion property of a cryptosystem measuring sensitivity of encryption results with respect to change of the secret key and the plaintext. The subtle similarity inspired researchers design secure multimedia encryption algorithms by combing chaos and cryptography.

*Corresponding author.
Email address: chengqingg@gmail.com (Chengqing Li)

Due to simple syntax of uncompress image and easy extension of image encryption scheme to other multimedia data, most chaos-based multimedia encryption scheme consider image data as encryption object. In the past decade, hundreds of chaos-based image encryption schemes have been proposed [1, 2]. In general, the usage of chaos in designing image encryption schemes can be categorized as the following three classes:

- creating position permutation matrices [1, 3, 4, 5];
- generating pseudo-random bit sequence, which is then used to control combination and composition of some basic arithmetical operations like modulo addition and exclusive or operation [6, 7, 8, 9, 10, 11, 12, 4].
- producing ciphertext directly when plain-bytes of image are converted to initial condition and control parameters of a chaotic map [13, 14].

Some general rules about evaluating security of chaos-based encryption algorithms can be found in [15].

In [16], a new image encryption algorithm using alternate structure (IEAS) based on the general cat-map and OCML (One-way Coupled Map Lattice) was proposed, where the two maps are used for realizing position permutation/diffusion and value substitution respectively. Essentially, structure of IEAS belongs to Feistel networks, i.e., an iterated block cipher where the output of the current round is determined by that of the previous one. This paper focuses on security analysis of IEAS and founds that some properties of IEAS, existing when its integer parameter is even, can be used to support a differential attack to recover equivalent secret key of IEAS with a little number of known/chosen plain-images. The detailed approaches of the differential attack are presented in detail when the round number of IEAS is less than or equal to four. In addition, the cryptanalysis also find some other security defects of IEAS, like insensitivity with respect to changes of plain-images and insufficiently large key space.

The rest of this paper is organized as follows. The next section introduces the image encryption algorithm under study, IEAS, briefly. Section 3 present the comprehensive cryptanalysis on the algorithm with some experiment results. The last section concludes the paper.

2. IEAS encryption algorithm

The plain-image encrypted by IEAS encryption algorithm is a gray-scale image of size $N \times 2N$ (height×width), which can be denoted by an $N \times 2N$ matrix in domain $\mathbb{Z}_{256}$. The encryption algorithm divides the plain-image into two parts of the same size: $\boldsymbol{L} = [L(i,j)]_{i=0,j=0}^{N-1,N-1}$ and $\boldsymbol{R} = [R(i,j)]_{i=0,j=0}^{N-1,N-1}$. The corresponding cipher-image is composed of two parts also: $\boldsymbol{l} = [l(i,j)]_{i=0,j=0}^{N-1,N-1}$ and $\boldsymbol{r} = [r(i,j)]_{i=0,j=0}^{N-1,N-1}$. With these notations, IEAS encryption algorithm can be described as follows[1].

- *The secret key*: the number of iteration round T and the initial condition $K_0 \in (0,1)$ of the chaotic Logistic map
$$\mathrm{f}(x) = \mu \cdot x \cdot (1-x).$$

[1]To make the presentation more concise and complete, some notations in the original paper [16] are modified, and some details about the algorithm are also supplied or corrected under precondition that its security is not influenced.

- *The initialization procedures*:

  1) run the Logistic map iteratively with fixed control parameter, $\mu = 4$, $T+2$ times from K_0 to generate a chaotic sequence $\{x_l\}_{l=0}^{T+1}$. Then, a 32-bit integer sequence $\{K_l\}_{l=0}^{T+1}$ is obtained from $\{x_l\}_{l=0}^{T+1}$ as

$$K_l = \lfloor x_l \cdot (2^{32} - 1) \rfloor.$$

  2) permute and expand the 32 binary bits of each element of $\{K_l\}_{l=0}^{T+1}$ by the look-up table shown in Table 1 and get a 50-bit integer sequence $\{K_l^*\}_{l=0}^{T+1}$.

Table 1: The Expansion Permutation Table.

32	1	2	3	4	5	4	5	6	7
8	9	8	9	10	11	12	13	14	15
16	17	16	17	15	16	17	18	19	20
21	20	21	22	23	24	25	24	25	26
27	28	29	28	29	30	31	32	1	31

  3) generate T permutation matrixes $\boldsymbol{P}_0 \sim \boldsymbol{P}_{T-1}$, whose every entry represents its sole location in the permuted version of the object to be permuted, as follows. For $l = 0 \sim T-1$, $i = 0 \sim N-1$, $j = 0 \sim N-1$, do

$$\boldsymbol{P}_l(i,j) = \boldsymbol{C}_l \cdot \begin{pmatrix} i \\ j \end{pmatrix} \bmod N, \tag{1}$$

  where $\boldsymbol{C}_l$ is the t-th element in the matrix set

$$\left\{ \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix}, \begin{pmatrix} ab+1 & a \\ b & 1 \end{pmatrix}, \begin{pmatrix} a & 1 \\ ab-1 & b \end{pmatrix}, \begin{pmatrix} a & ab-1 \\ 1 & b \end{pmatrix} \right\}, \tag{2}$$

  $t = \sum_{k=0}^{1} K_{l,k}^* \cdot 2^k$, $a = \sum_{k=0}^{7} K_{l,k+2}^* \cdot 2^k$, $b = \sum_{k=0}^{7} K_{l,k+10}^* \cdot 2^k$, $K_l^* = \sum_{k=0}^{49} K_{l,k}^* \cdot 2^k$.

  4) produce $T+2$ mask matrixes, $\boldsymbol{V}_0 \sim \boldsymbol{V}_{T+1}$, of size $N \times N$ with the following two steps.

  - Utilize an OCML model to generate $T+2$ pseudo-random number matrixes of size $N \times N$, $\boldsymbol{W}_0 \sim \boldsymbol{W}_{T+1}$. For $i = 0 \sim N-1$, $j = 0 \sim N-1$, do

$$\boldsymbol{W}_l(i,j) = (1-\varepsilon) \cdot f(\boldsymbol{W}_l(i,j-1)) + \varepsilon \cdot f(\boldsymbol{W}_l(i-1,j-1)),$$

    where $\varepsilon = 0.875$, and the boundary conditions, $\boldsymbol{W}_l(-1,-1) \sim \boldsymbol{W}_l(-1,N-1)$ and $\boldsymbol{W}_l(0,-1) \sim \boldsymbol{W}_l(N-2,-1)$, are assigned by the chaotic states obtained by iterating the Logistic map $2N$ times from initial condition $(\sum_{k=0}^{31} K_{l,k+18}^* \cdot 2^k)/2^{32}$.
  - Discretize $\boldsymbol{W}_0 \sim \boldsymbol{W}_{T+1}$ into $\boldsymbol{V}_0 \sim \boldsymbol{V}_{T+1}$. For $i = 0 \sim N-1$, $j = 0 \sim N-1$, do

$$\boldsymbol{V}_l(i,j) = \lfloor \boldsymbol{W}_l(i,j) \cdot 256 \rfloor.$$

- *The encryption procedure* is composed of T rounds of five main steps. Let $\boldsymbol{L}_l$ and $\boldsymbol{R}_l$ denote the left half part and the right half part of intermediate data obtained in the l-th round of encryption, respectively. The schematic structure of IEAS is shown in Fig. 1. Set $l = 0$, $\boldsymbol{L}_l = \boldsymbol{L}$ and $\boldsymbol{R}_l = \boldsymbol{R}$, IEAS runs with the following five steps repeatedly.

– *Step (a) mask substitution on the left half part in the current round*: let $l = l + 1$, and do

$$\boldsymbol{R}_l(i,j) = \boldsymbol{V}_{l-1}(i,j) \oplus \boldsymbol{L}_{l-1}(i,j) \tag{3}$$

for $i = 0 \sim N-1$, $j = 0 \sim N-1$.

– *Step (b) permutation on the right half part in the next round*: for $i = 0 \sim N-1$, $j = 0 \sim N-1$, do

$$\widetilde{\boldsymbol{R}}_l(i,j) = \boldsymbol{R}_l(\boldsymbol{P}_{l-1}(i,j)).$$

For simplicity, $\boldsymbol{R}_l(\boldsymbol{P}_{l-1})$ denotes this operation in remainder of this paper.

– *Step (c) substitution on the permuted right part*: for $k = 1 \sim N^2 - 1$, do

$$\boldsymbol{L}_l(i,j) = \boldsymbol{R}_{l-1}(i,j) \oplus \mathrm{g}\left(\widetilde{\boldsymbol{R}}_l(i,j), \widetilde{\boldsymbol{R}}_l(i',j')\right), \tag{4}$$

where $\boldsymbol{L}_l(0,0) = \boldsymbol{R}_{l-1}(0,0) \oplus \widetilde{\boldsymbol{R}}_l(0,0)$, $i = \lfloor k/N \rfloor$, $j = \mathrm{mod}(k,N)$, $i' = \lfloor k-1/N \rfloor$, $j' = \mathrm{mod}(k-1,N)$, and

$$\mathrm{g}(x,y) = (x + A * y) \bmod 256. \tag{5}$$

– *Step (d) repetition*: repeat *Step (a)* through *Step (c)* $T-1$ times.

– *Step (e) final mask substitution*: generate the two half parts of cipher-image as follows: do

$$\boldsymbol{r} = \boldsymbol{V}_T \oplus \boldsymbol{L}_T \tag{6}$$

and

$$\boldsymbol{l} = \boldsymbol{V}_{T+1} \oplus \boldsymbol{R}_T, \tag{7}$$

where the exclusive or operation between two matrixes is calculated element-wise, the same hereinafter.

- *The decryption procedure* is similar to the encryption process except the following simple modifications: 1) the *Step (e)* is performed first; 2) the different rounds of encryption are exerted in a reverse order.

3. Differential cryptanalysis

Task of differential cryptanalysis is to get information of (equivalent) secret key of an encryption algorithm by observing how differences in an input can affect the resultant ones at the output. Generally, the difference is defined with respect to exclusive or (XOR) operation. In the following, some properties of IEAS are introduced first, which works as basis for differential attack on IEAS under different round numbers.

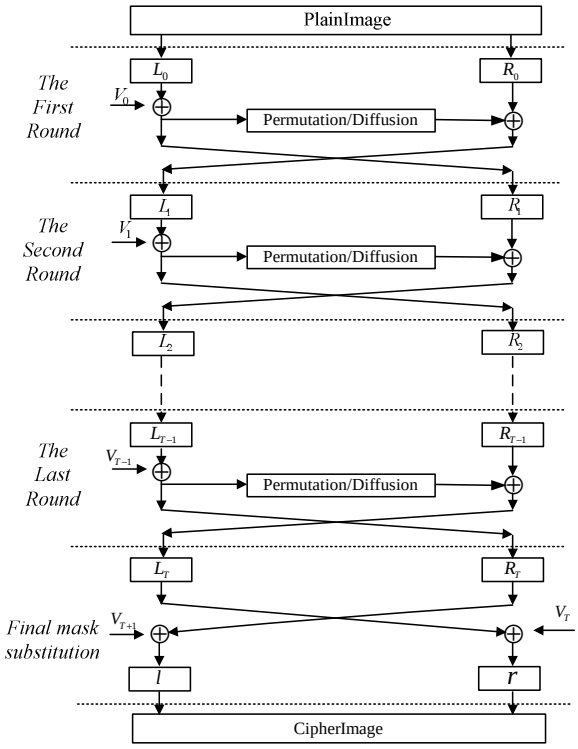

Figure 1: Schematic structure of IEAS.

3.1. Some properties of IEAS

Property 1. *Given two matrix entries* (i_1, j_1) *and* (i_2, j_2) *in* $\boldsymbol{R}_l$*, and let* $(\tilde{i}_1, \tilde{j}_1)$ *and* $(\tilde{i}_2, \tilde{j}_2)$ *denote the corresponding locations in* $\widetilde{\boldsymbol{R}}_l$*. If the two original entries satisfy*

$$\gcd(\Delta, N) = 1, \tag{8}$$

one has

$$\boldsymbol{C}_l = \begin{pmatrix} s & u \\ v & t \end{pmatrix},$$

where

$$\begin{pmatrix} s \\ u \\ v \\ t \end{pmatrix} = \begin{pmatrix} \Delta^{-1}(\tilde{i}_1 j_2 - \tilde{i}_2 j_1) \\ \Delta^{-1}(\tilde{i}_2 i_1 - \tilde{i}_1 i_2) \\ \Delta^{-1}(\tilde{j}_1 j_2 - \tilde{j}_2 j_1) \\ \Delta^{-1}(\tilde{j}_2 i_1 - \tilde{j}_1 i_2) \end{pmatrix} \bmod N,$$

$\Delta = i_1 j_2 - i_2 j_1$*, and* $\Delta \cdot \Delta^{-1} = 1 \bmod N$.

Proof. Obviously, (i_1, j_1), (i_2, j_2), $(\tilde{i}_1, \tilde{j}_1)$, and $(\tilde{i}_2, \tilde{j}_2)$ satisfy

$$\begin{pmatrix} si_1 + uj_1 \\ si_2 + uj_2 \end{pmatrix} \bmod N = \begin{pmatrix} \tilde{i}_1 \\ \tilde{i}_2 \end{pmatrix},$$

which means

$$\begin{pmatrix} i_1 & j_1 \\ i_2 & j_2 \end{pmatrix} \cdot \begin{pmatrix} s \\ u \end{pmatrix} = \begin{pmatrix} \tilde{i}_1 + K_1 N \\ \tilde{i}_2 + K_2 N \end{pmatrix},$$

where $K_1, K_2 \in \mathbb{Z}$.

Use the Gaussian elimination method, one can get

$$\begin{pmatrix} i_1 & j_1 \\ 0 & i_1 j_2 - i_2 j_1 \end{pmatrix} \cdot \begin{pmatrix} s \\ u \end{pmatrix} = \begin{pmatrix} \tilde{i}_1 + K_1 N \\ i_1 \tilde{i}_2 - i_2 \tilde{i}_1 + N(K_2 i_1 - K_1 i_2) \end{pmatrix}.$$

According to the Cramer's rule, the above equation have one and only one solution when $\gcd(\Delta, N) = 1$. Thus,

$$\begin{aligned} s &= \Delta^{-1}(\tilde{i}_1 j_2 - \tilde{i}_2 j_1) \bmod N, \\ u &= \Delta^{-1}(\tilde{i}_2 i_1 - \tilde{i}_1 i_2) \bmod N. \end{aligned}$$

The value of v, t can be obtained similarly. □

Property 2. *If 2^n $(1 \le n \le 7)$ divides variable A in Eq. (5), then the substitution function $\mathrm{g}(x, y)$ has no influence on the n least significant bits of x, i.e., Eq. (4) becomes*

$$\boldsymbol{L}_{l,k}(i, j) = \boldsymbol{R}_{l-1,k}(i, j) \oplus \widetilde{\boldsymbol{R}}_{l,k}(i, j),$$

where $k \in \{1, \cdots, n\}$, $\boldsymbol{L}_{l,k}$, $\boldsymbol{R}_{l-1,k}$ and $\widetilde{\boldsymbol{R}}_{l,k}$ are the k-th least significant bit plane of $\boldsymbol{L}_l$, $\boldsymbol{R}_{l-1}$, and $\widetilde{\boldsymbol{R}}_l$, respectively.

Proof. This property can be easily proved by calculating

$$\begin{aligned} \mathrm{g}(x, y) &= x + A \cdot \sum_{i=0}^{7} y_i 2^i \bmod 256 \\ &= x + (A/2^n) \cdot \sum_{i=n}^{7} y_i 2^i \bmod 256. \end{aligned}$$

□

Let $\boldsymbol{L}'_l$, $\boldsymbol{R}'_l(\boldsymbol{P}_{l-1})$ and $\boldsymbol{R}'_{l-1}$ denote differential of two versions of $\boldsymbol{L}_l$, $\boldsymbol{R}_l(\boldsymbol{P}_{l-1})$ and $\boldsymbol{R}_{l-1}$, respectively. Observe the structure of intermediate data under different rounds shown in Fig. 2, we can get the following property.

Property 3. *If 2^n $(1 \le n \le 7)$ divides variable A in Eq. (5), one has*

$$\begin{cases} \boldsymbol{R}'_l = \boldsymbol{L}'_{l-1}, \\ \boldsymbol{L}'_{l,k} = \boldsymbol{R}'_{l-1,k} \oplus \boldsymbol{R}'_{l,k}(\boldsymbol{P}_{l-1}), \end{cases}$$

where $k \in \{1, \cdots, n\}$, $\boldsymbol{L}'_{l,k}$, $\boldsymbol{R}'_{l-1,k}$ and $\boldsymbol{R}'_{l,k}(\boldsymbol{P}_{l-1})$ are the k-th least significant bit plane of $\boldsymbol{L}'_l$, $\boldsymbol{R}'_{l-1}$ and $\boldsymbol{R}'_l(\boldsymbol{P}_{l-1})$, respectively.

Proof. This property can be easily proved with mathematical induction on l ($1 \leq l \leq T$). When $l = 1$,

$$\begin{aligned}
\boldsymbol{R}'_1 &= \boldsymbol{R}_1 \oplus \boldsymbol{R}^*_1 \\
&= (\boldsymbol{L}_0 \oplus \boldsymbol{V}_0) \oplus (\boldsymbol{L}^*_0 \oplus \boldsymbol{V}_0) \\
&= \boldsymbol{L}'_0, \\
\boldsymbol{L}'_{1,k} &= (\boldsymbol{R}_{0,k} \oplus \boldsymbol{R}_{1,k}(\boldsymbol{P}_0)) \oplus (\boldsymbol{R}^*_{0,k} \oplus \boldsymbol{R}^*_{1,k}(\boldsymbol{P}_0)) \\
&= \boldsymbol{R}'_{0,k} \oplus \boldsymbol{R}'_{1,k}(\boldsymbol{P}_0).
\end{aligned}$$

So, the property holds for $l = 1$. Assume that the property is true for $l = n$ ($n < T$), we prove the case for $l = n + 1$.

$$\begin{aligned}
\boldsymbol{R}'_{n+1} &= (\boldsymbol{L}_n \oplus \boldsymbol{V}_n) \oplus (\boldsymbol{L}^*_n \oplus \boldsymbol{V}_n) \\
&= \boldsymbol{L}'_n, \\
\boldsymbol{L}'_{n+1,k} &= (\boldsymbol{R}_{n,k} \oplus \boldsymbol{R}_{n+1,k}(\boldsymbol{P}_n)) \oplus (\boldsymbol{R}^*_{n,k} \oplus \boldsymbol{R}^*_{n+1,k}(\boldsymbol{P}_n)) \\
&= \boldsymbol{R}'_{n,k} \oplus \boldsymbol{R}'_{n+1,k}(\boldsymbol{P}_n).
\end{aligned}$$

This completes the mathematical induction. □

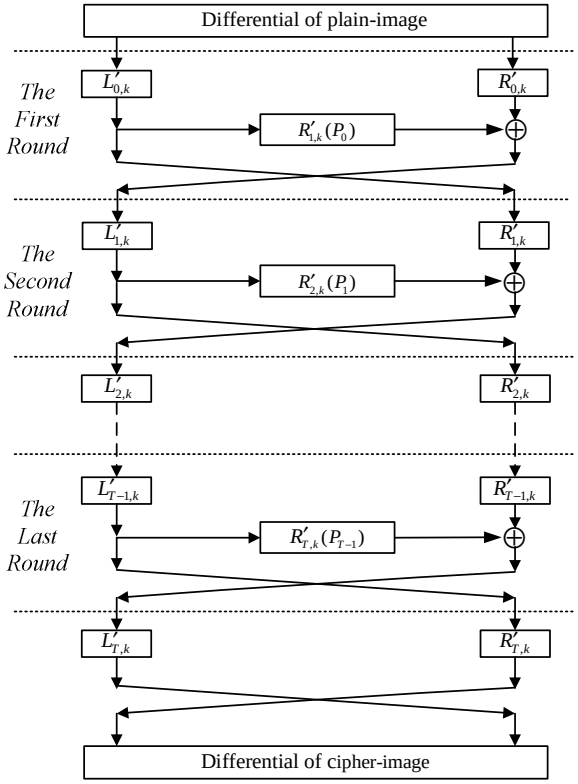

Figure 2: Schematic structure of differential of intermediate data under different rounds.

3.2. Breaking IEAS when the number of iteration round is equal to one

Given two known/chosen plain-images, $[\boldsymbol{L}_0, \boldsymbol{R}_0]$ and $[\boldsymbol{L}_0^*, \boldsymbol{R}_0^*]$, and the corresponding cipher-images, $[\boldsymbol{l}, \boldsymbol{r}]$ and $[\boldsymbol{l}^*, \boldsymbol{r}^*]$, one has

$$\begin{cases} \boldsymbol{L}_0' = \boldsymbol{L}_0 \oplus \boldsymbol{L}_0^*, \\ \boldsymbol{R}_0' = \boldsymbol{R}_0 \oplus \boldsymbol{R}_0^*, \end{cases}$$

and

$$\begin{cases} \boldsymbol{L}_1' = \boldsymbol{r} \oplus \boldsymbol{r}^*, \\ \boldsymbol{R}_1' = \boldsymbol{l} \oplus \boldsymbol{l}^*. \end{cases}$$

From Property 3, one can get

$$\begin{cases} \boldsymbol{R}_1' = \boldsymbol{L}_0', \\ \boldsymbol{R}_{1,k}'(\boldsymbol{P}_0) = \boldsymbol{L}_{1,k}' \oplus \boldsymbol{R}_{0,k}', \end{cases} \tag{9}$$

where $k \in \{1, \cdots, n\}$, 2^n $(1 \leq n \leq 7)$ divides the parameter A in Eq. (5). Comparing $\{\boldsymbol{R}_{1,k}'\}_{k=1}^n$ and $\{\boldsymbol{R}_{1,k}'(\boldsymbol{P}_0)\}_{k=1}^n$, one may find two pairs of entries in $\boldsymbol{R}_1'$ and $\boldsymbol{R}_1'(\boldsymbol{P}_0)$ whose locations satisfying condition (8). Then, the transformation matrix $\boldsymbol{C}_0$, generating the associated permutation matrix $\boldsymbol{P}_0$, can be solved according to Property 1. In case the search of the required entries failed, one can resort to observing more known plain-images or constructing special differential images from more chosen plain-images [5]. As shown in [5], $\lceil 2\log_2(N) \rceil$ chosen binary plain-images are enough to break any position permutation-only encryption algorithm exerting on binary plain-images of size $N \times N$. Due to similarity, we do not mention the problem about determining permutation matrix with more known/chosen plain-images in the remainder of this paper. Once $\boldsymbol{C}_0$ is determined, the associated matrix $\boldsymbol{P}_0$ can be obtained from it easily.

Referring to Eq. (3) and Eq. (7), one can get

$$\boldsymbol{V}_2 \oplus \boldsymbol{V}_0 = \boldsymbol{L}_0 \oplus \boldsymbol{l}. \tag{10}$$

Combining Eq. (6) and Eq. (4) yields

$$\boldsymbol{r}_k = \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{R}_{1,k}(\boldsymbol{P}_0), \tag{11}$$

where $\boldsymbol{r}_k$ is the k-th least significant bit plane of $\boldsymbol{r}$. As the exclusive or operation is linear with respect to position permutation, one can get

$$\boldsymbol{R}_{1,k}(\boldsymbol{P}_0) = \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0)$$

from Eq. (3). Substitute $\boldsymbol{R}_{1,k}(\boldsymbol{P}_0)$ obtained in the above equation into Eq. (11), one can further get

$$\boldsymbol{V}_{1,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) = \boldsymbol{r}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0). \tag{12}$$

Since neither of Eq. (10) and Eq. (12) has any special requirement on the pair of plain-image and corresponding cipher-image, some parts of any other cipher-image encrypted with the same secret key, $[\boldsymbol{l}^\star, \boldsymbol{r}^\star]$, can be recovered by calculating

$$\begin{cases} \boldsymbol{L}_0^\star = \boldsymbol{l}^\star \oplus \boldsymbol{M}_1, \\ \boldsymbol{R}_{0,k}^\star = \boldsymbol{r}_k^\star \oplus \boldsymbol{L}_{0,k}^\star(\boldsymbol{P}_0) \oplus \boldsymbol{N}_{1,k}, \end{cases}$$

where

$$\begin{cases} \boldsymbol{M}_1 = \boldsymbol{L}_0 \oplus \boldsymbol{l}, \\ \boldsymbol{N}_{1,k} = \boldsymbol{r}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0). \end{cases}$$

Now, one can see that $\boldsymbol{M}_1$, $\{\boldsymbol{N}_{1,k}\}_{k=1}^n$ and $\boldsymbol{P}_0$ can work together to recover the whole left half part of $\boldsymbol{l}^\star$, and the n least significant bit planes of the right part of $\boldsymbol{r}^\star$, $\{\boldsymbol{R}_{0,k}^\star\}_{k=1}^n$.

To verify the above analysis, some experiments on some plain-images of size 256×512 are made. With secret key $K_0 = 1234567/(2^{32}-1)$, $T = 1$ and parameter $A = 64$, two known plain-images, cropped version of two standard images, "Lenna" and "Baboon", and the corresponding cipher-images are shown in Figs. 3a), b), d), e), respectively. The obtained information about the secret key is used to decrypt another cipher-image shown in Fig. 3c), and result is shown in Fig. 3f). The whole left half part and the 6 least significant bit planes of the right half part of the recovered image shown in Fig. 3f) are identical with counterpart of the corresponding plain-image, which agree with the expected result well.

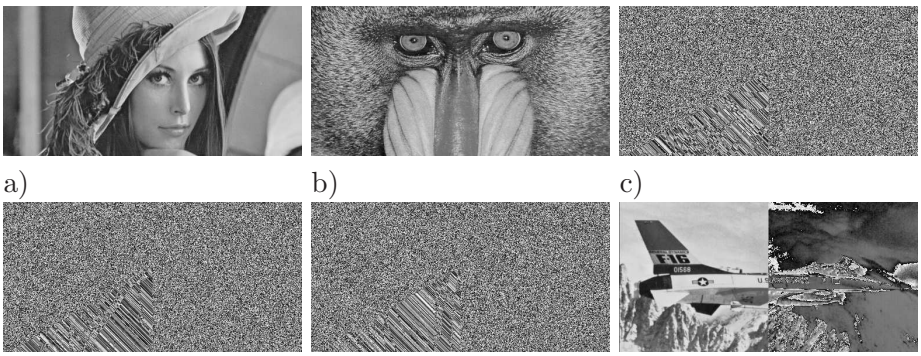

Figure 3: Differential attack on IEAS when $T = 1$: a) the first known plain-image; b) the second known plain-image; c) cipher-image of plain-image "Airplane"; d) cipher-image of Fig. 3a); e) cipher-image of Fig. 3b); f) the recovered plain-image of Fig. 3c).

3.3. Breaking IEAS when the number of iteration round is equal to two

In this case, the differential of ciphertext is

$$\begin{cases} \boldsymbol{L}_2' = \boldsymbol{r} \oplus \boldsymbol{r}^*, \\ \boldsymbol{R}_2' = \boldsymbol{l} \oplus \boldsymbol{l}^*. \end{cases} \tag{13}$$

From Property 3, one has

$$\begin{cases} \boldsymbol{R}_1' = \boldsymbol{L}_0', \\ \boldsymbol{R}_{1,k}'(\boldsymbol{P}_0) = \boldsymbol{R}_{2,k}' \oplus \boldsymbol{R}_{0,k}', \end{cases}$$

where $\boldsymbol{R}_{2,k}'$ is the k-th least significant bit plane of $\boldsymbol{R}_2'$. Then, the transformation matrix $\boldsymbol{C}_0$, generating the associated permutation matrix $\boldsymbol{P}_0$, can be recovered by comparing $\{\boldsymbol{R}_{1,k}'\}_{k=1}^n$ and $\{\boldsymbol{R}_{1,k}'(\boldsymbol{P}_0)\}_{k=1}^n$.

Still from Property 3, one has

$$\begin{aligned} \boldsymbol{R}_{2,k}'(\boldsymbol{P}_1) &= \boldsymbol{L}_{2,k}' \oplus \boldsymbol{R}_{1,k}' \\ &= \boldsymbol{L}_{2,k}' \oplus \boldsymbol{L}_{0,k}'. \end{aligned}$$

Similarly, one can get the transform matrix $\boldsymbol{C}_1$, then permutation matrix $\boldsymbol{P}_1$, by comparing $\{\boldsymbol{R}'_{2,k}\}_{k=1}^n$ and $\{\boldsymbol{R}'_{2,k}(\boldsymbol{P}_1)\}_{k=1}^n$.

Referring to Eq. (7), one has

$$\boldsymbol{l}_k = \boldsymbol{V}_{3,k} \oplus \boldsymbol{R}_{2,k}, \tag{14}$$

where $\boldsymbol{l}_k$ is the k-th least significant bit plane of $\boldsymbol{l}$. Combining Eq. (3), Eq. (4) and Eq. (6) yields

$$\begin{aligned}\boldsymbol{r}_k &= \boldsymbol{V}_{2,k} \oplus \boldsymbol{L}_{2,k} \\ &= \boldsymbol{V}_{2,k} \oplus \boldsymbol{R}_{1,k} \oplus \boldsymbol{R}_{2,k}(\boldsymbol{P}_1) \\ &= \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{R}_{2,k}(\boldsymbol{P}_1).\end{aligned}$$

Substitute $\boldsymbol{R}_{2,k}$ obtained in Eq. (14) into the above equation, one has

$$\boldsymbol{V}_{3,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} = \boldsymbol{l}_k(\boldsymbol{P}_1) \oplus \boldsymbol{r}_k \oplus \boldsymbol{L}_{0,k}. \tag{15}$$

Combine Eq. (3) and Property 2, one can get

$$\begin{aligned}\boldsymbol{R}_{2,k} &= \boldsymbol{V}_{1,k} \oplus \boldsymbol{L}_{1,k} \\ &= \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{R}_{1,k}(\boldsymbol{P}_0) \\ &= \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0),\end{aligned} \tag{16}$$

then Eq. (14) becomes

$$\boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) = \boldsymbol{l}_k \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{R}_{0,k}. \tag{17}$$

Since both Eq. (15) and Eq. (17) always hold for any pair of plain-image and cipher-image encrypted with the same secret key, it can be easily verified that

$$\begin{cases}\boldsymbol{L}^\star_{0,k} = \boldsymbol{l}^\star_k(\boldsymbol{P}_1) \oplus \boldsymbol{r}^\star_k \oplus \boldsymbol{M}_{2,k}, \\ \boldsymbol{R}^\star_{0,k} = \boldsymbol{l}^\star_k \oplus \boldsymbol{L}^\star_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{N}_{2,k},\end{cases}$$

where

$$\begin{cases}\boldsymbol{M}_{2,k} = \boldsymbol{l}_k(\boldsymbol{P}_1) \oplus \boldsymbol{r}_k \oplus \boldsymbol{L}_{0,k}, \\ \boldsymbol{N}_{2,k} = \boldsymbol{l}_k \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{R}_{0,k}.\end{cases}$$

The above equations mean that $\boldsymbol{M}_{2,k}$, $\boldsymbol{N}_{2,k}$ and $\{\boldsymbol{P}_l\}_{l=0}^1$ can work together to recover the k-th least significant bit plane of any other cipher-image encrypted with the same secret key, $[\boldsymbol{L}^\star_{0,k}, \boldsymbol{R}^\star_{0,k}]$, for $k = 1 \sim n$.

To verify the above analysis, some experiments are made. With secret key $K_0 = 1234567/(2^{32} - 1)$, $T = 2$ and parameter $A = 64$, encryption results of the two known-images shown in Figs. 3a) and b) are shown in Figs. 4a) and b), respectively. The information about equivalent secret key obtained from the two pairs of plain-images and cipher-images is used decrypt another cipher-image shown in Fig. 4c) and the result is shown in Fig. 4d). It is counted that the 6 least significant bit planes of the image shown in Fig. 4d) are identical with the counterparts of the corresponding plain-image.

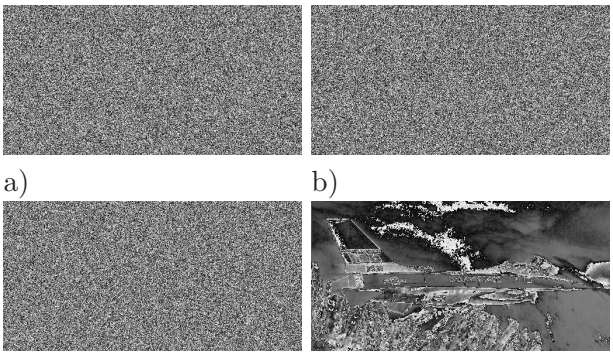

Figure 4: Differential attack on IEAS when $T = 2$: a) cipher-image of Fig. 3a); b) cipher-image of Fig. 3b); c) cipher-image of plain-image "Airplane"; d) the recovered plain-image of Fig. 4c).

3.4. Breaking IEAS when the round number is equal to three

In this sub-section we discuss how to break the version of IEAS of three rounds with no less than three chosen plain-images.

In this case, the differential of ciphertext is

$$\begin{cases} \boldsymbol{L}'_3 = \boldsymbol{r} \oplus \boldsymbol{r}^*, \\ \boldsymbol{R}'_3 = \boldsymbol{l} \oplus \boldsymbol{l}^*. \end{cases}$$

According to Property 3, one has

$$\begin{aligned} \boldsymbol{L}'_{3,k} &= \boldsymbol{R}'_{3,k}(\boldsymbol{P}_2) \oplus \boldsymbol{R}'_{2,k} \\ &= \boldsymbol{R}'_{3,k}(\boldsymbol{P}_2) \oplus \boldsymbol{R}'_{0,k} \oplus \boldsymbol{R}'_{1,k}(\boldsymbol{P}_0) \\ &= \boldsymbol{R}'_{3,k}(\boldsymbol{P}_2) \oplus \boldsymbol{R}'_{0,k} \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_0). \end{aligned} \tag{18}$$

If $\boldsymbol{L}'_{0,k}$ is chosen as a binary matrix of fixed value, which makes

$$\boldsymbol{L}'_{0,k}(\boldsymbol{P}_0) \equiv \boldsymbol{L}'_{0,k}, \tag{19}$$

$\boldsymbol{R}'_{3,k}(\boldsymbol{P}_2)$ can be obtained from Eq. (18). With the same method mentioned above, $\boldsymbol{P}_2$ can be recovered by comparing $\{\boldsymbol{R}'_{3,k}\}_{k=1}^n$ and $\{\boldsymbol{R}'_{3,k}(\boldsymbol{P}_2)\}_{k=1}^n$.

As for the differential image satisfying Eq. (19), one also has

$$\begin{aligned} \boldsymbol{R}'_{2,k} &= \boldsymbol{R}'_{3,k}(\boldsymbol{P}_2) \oplus \boldsymbol{L}'_{3,k} \\ &= \boldsymbol{R}'_{0,k} \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_0) \\ &= \boldsymbol{R}'_{0,k} \oplus \boldsymbol{L}'_{0,k}. \end{aligned} \tag{20}$$

Note that

$$\begin{aligned} \boldsymbol{R}'_{3,k} &= \boldsymbol{L}'_{2,k} \\ &= \boldsymbol{R}'_{1,k} \oplus \boldsymbol{R}'_{2,k}(\boldsymbol{P}_1). \end{aligned}$$

Substitute Eq. (20) into the above equation, one can get

$$\begin{aligned}\boldsymbol{R}'_{3,k} &= \boldsymbol{R}'_{1,k} \oplus \boldsymbol{R}'_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_1)\\ &= \boldsymbol{L}'_{0,k} \oplus \boldsymbol{R}'_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{L}'_{0,k}\\ &= \boldsymbol{R}'_{0,k}(\boldsymbol{P}_1).\end{aligned}$$

Then, $\boldsymbol{R}'_{0,k}(\boldsymbol{P}_1)$ can be obtained from the above equation, and $\boldsymbol{P}_1$ can be recovered by comparing $\{\boldsymbol{R}'_{0,k}\}_{k=1}^{n}$ and $\{\boldsymbol{R}'_{0,k}(\boldsymbol{P}_1)\}_{k=1}^{n}$.

Once $\boldsymbol{P}_2$ is recovered, $\boldsymbol{L}'_{0,k}(\boldsymbol{P}_0)$ can be obtained from Eq. (18). Then, $\boldsymbol{P}_0$ can be recovered by comparing $\{\boldsymbol{L}'_{0,k}\}_{k=1}^{n}$ and $\{\boldsymbol{L}'_{0,k}(\boldsymbol{P}_0)\}_{k=1}^{n}$. As mentioned before, one and even more pairs of plaintext and the corresponding ciphertexts are required to find two pairs of entries in $\boldsymbol{L}'_{0,k}$ and $\boldsymbol{L}'_{0,k}(\boldsymbol{P}_0)$ whose locations satisfying condition (8).

From Eq. (7), one has

$$\boldsymbol{l}_k = \boldsymbol{V}_{4,k} \oplus \boldsymbol{R}_{3,k}, \tag{21}$$

where $\boldsymbol{R}_{3,k}$ is the k-th least significant bit plane of $\boldsymbol{R}_3$. Combine Eq. (3), Eq. (4) and Eq. (6), one can get

$$\begin{aligned}\boldsymbol{r}_k &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{L}_{3,k}\\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{R}_{2,k} \oplus \boldsymbol{R}_{3,k}(\boldsymbol{P}_2)\\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{L}_{1,k} \oplus \boldsymbol{R}_{3,k}(\boldsymbol{P}_2)\\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{R}_{1,k}(\boldsymbol{P}_0) \oplus \boldsymbol{R}_{3,k}(\boldsymbol{P}_2)\\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{R}_{3,k}(\boldsymbol{P}_2).\end{aligned}$$

Substitute $\boldsymbol{R}_{3,k}$ obtained in Eq. (21) into the above equation and get

$$\boldsymbol{V}_{4,k}(\boldsymbol{P}_2) \oplus \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) = \boldsymbol{l}_k(\boldsymbol{P}_2) \oplus \boldsymbol{r}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0). \tag{22}$$

Referring to Eq. (3) and Eq. (16), one has

$$\begin{aligned}\boldsymbol{R}_{3,k} &= \boldsymbol{V}_{2,k} \oplus \boldsymbol{L}_{2,k}\\ &= \boldsymbol{V}_{2,k} \oplus \boldsymbol{R}_{1,k} \oplus \boldsymbol{R}_2(\boldsymbol{P}_1)\\ &= \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1),\end{aligned} \tag{23}$$

then Eq. (21) can be rewritten as

$$\boldsymbol{l}_k = \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1).$$

Substitute $\boldsymbol{L}_{0,k}(\boldsymbol{P}_0)$ obtained in Eq. (22) into the above equation, and get

$$\boldsymbol{V}_{4,k}(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{V}_{3,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} = \boldsymbol{l}_k(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{r}_k(\boldsymbol{P}_1) \oplus \boldsymbol{l}_k \oplus \boldsymbol{L}_{0,k}. \tag{24}$$

Since both Eq. (22) and Eq. (24) hold for any pair of plain-image and its corresponding cipher-image, it can be easily verified that

$$\begin{cases} \boldsymbol{L}^{\star}_{0,k} = \boldsymbol{l}^{\star}_k(\boldsymbol{P_2}\boldsymbol{P_1}) \oplus \boldsymbol{r}^{\star}_k(\boldsymbol{P_1}) \oplus \boldsymbol{l}^{\star}_k \oplus \boldsymbol{M}_{3,k},\\ \boldsymbol{R}^{\star}_{0,k} = \boldsymbol{l}^{\star}_k(\boldsymbol{P_2}) \oplus \boldsymbol{r}^{\star}_k \oplus \boldsymbol{L}^{\star}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{N}_{3,k}, \end{cases}$$

where

$$\begin{cases} \boldsymbol{M}_{3,k} = \boldsymbol{l}_k(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{r}_k(\boldsymbol{P}_1) \oplus \boldsymbol{l}_k \oplus \boldsymbol{L}_{0,k}, \\ \boldsymbol{N}_{3,k} = \boldsymbol{l}_k(\boldsymbol{P}_2) \oplus \boldsymbol{r}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0). \end{cases}$$

The above equations mean that $\boldsymbol{M}_{3,k}$, $\boldsymbol{N}_{3,k}$ and $\{\boldsymbol{P}_l\}_{l=0}^2$ can work together to recover the k-th least significant bit plane of any other cipher-image encrypted with the same secret key, $[\boldsymbol{L}_{0,k}^\star, \boldsymbol{R}_{0,k}^\star]$, for $k = 1 \sim n$.

To verify the above analysis, some similar experiments are made with $K_0 = 1234567/(2^{32}-1)$, $T = 3$ and $A = 64$. First, a chosen plain-image is composed by combining the left half part of Fig. 3a) and the right half part of Fig. 3b), which makes the special differential files satisfying Eq. (19) can be generated. Then, the three plain-images shown in Figs. 3a), b), Fig. 5a) and a plain-image "Airplane" are encrypted with the same secret key, and the results are shown in Figs. 5b), c), d), e), respectively. With the three pairs of plain-images and cipher-images, some information about the secret key is obtained to decrypt the cipher-image shown in Fig. 5e) and the result is shown in Fig. 5f). It is counted that the 6 least significant bit planes of the image shown in Fig. 5f) are identical with the counterparts of the corresponding plain-image also.

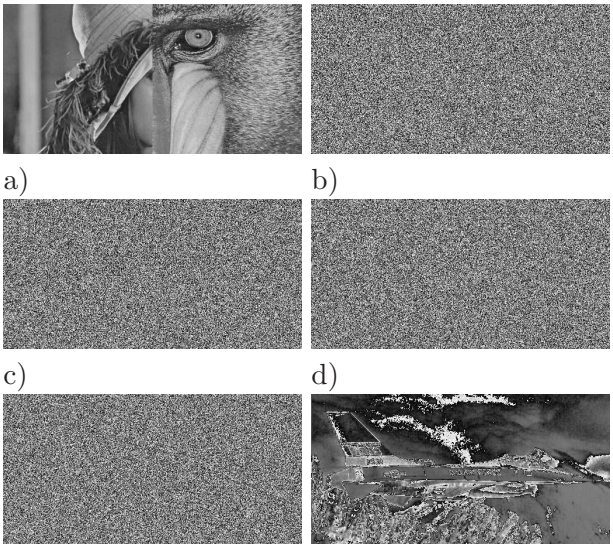

Figure 5: Differential attack on IEAS when $T = 3$: a) the constructed plain-image; b) cipher-image of Fig. 3a); c) cipher-image of Fig. 3b); d) cipher-image of Fig. 5a); e) cipher-image of the plain-image "Airplane"; f) the recovered plain-image of Fig. 5e).

3.5. Breaking IEAS of higher rounds ($T \geq 4$)

It is not hard to notice that there are some general approaches to breaking IEAS of different rounds. Here, we take breaking the version of IEAS under four rounds as an example to illustrate how to implement differential attack on IEAS in a general way.

- *Step 1) breaking position permutation*:

According to Property 3, one has

$$\begin{aligned}\boldsymbol{L}'_{4,k} &= \boldsymbol{R}'_{4,k}(\boldsymbol{P}_3) \oplus \boldsymbol{R}'_{3,k} \\ &= \boldsymbol{L}'_{3,k}(\boldsymbol{P}_3) \oplus \boldsymbol{L}'_{2,k} \\ &= \boldsymbol{R}'_{2,k}(\boldsymbol{P}_3) \oplus \boldsymbol{L}'_{2,k}(\boldsymbol{P}_2\boldsymbol{P}_3) \oplus \boldsymbol{R}'_{2,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}'_{1,k} \\ &= \boldsymbol{R}'_{0,k}(\boldsymbol{P}_3) \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_3) \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_2\boldsymbol{P}_3) \oplus \boldsymbol{L}'_{1,k}(\boldsymbol{P}_1\boldsymbol{P}_2\boldsymbol{P}_3) \\ &\quad \oplus \boldsymbol{R}'_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \oplus \boldsymbol{L}'_{0,k}, \end{aligned} \tag{25}$$

and $\boldsymbol{L}'_{1,k} = \boldsymbol{R}'_{0,k} \oplus \boldsymbol{R}'_{1,k}(\boldsymbol{P}_0)$, where $\boldsymbol{R}'_{4,k}$ is the k-th least significant bit plane of $\boldsymbol{R}'_4$. Then, the problem become how to recover the permutation matrixes generated by Eq. (1) by constructing some special differential plain-images.

– *Determining $\boldsymbol{P}_1$ and $\boldsymbol{P}_3$ by choosing special $\boldsymbol{R}'_{0,k}$*
If $\boldsymbol{L}'_{0,k}$ is chosen of fixed value zero, one can get $\boldsymbol{L}'_{1,k} = \boldsymbol{R}'_{0,k}$. Substitute it into Eq. (25), one has

$$\boldsymbol{L}'_{4,k} = \boldsymbol{R}'_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}'_{0,k}(\boldsymbol{P}_3) \oplus \boldsymbol{R}'_{0,k}(\boldsymbol{P}_1\boldsymbol{P}_2\boldsymbol{P}_3). \tag{26}$$

Assume a special differential image satisfy $\boldsymbol{L}'_{0,k}(i,j) \equiv 0$ and $\boldsymbol{R}'_{0,k}(i,j) = 0$ except that

$$\begin{cases} \boldsymbol{R}'_{0,k}(i_1, j_1) = \alpha_1, \\ \boldsymbol{R}'_{0,k}(i_2, j_2) = \beta_1, \end{cases} \tag{27}$$

where $\gcd(i_1 j_2 - i_2 j_1, N) = 1$ and $\alpha_1 \neq \beta_1$. Observe Eq. (26), one can see that one pixel of $\boldsymbol{R}'_{0,k}$ can influence at most three pixels of $\boldsymbol{L}'_{4,k}$. So, one can get $\binom{3}{1} \cdot \binom{3-1}{1} = 6$ possible values of $(\boldsymbol{C}_1, \boldsymbol{C}_3, \boldsymbol{C}_1\boldsymbol{C}_2\boldsymbol{C}_3)$ by referring to Property 1. When condition of Proposition 1 exist, the matrix $(\boldsymbol{C}_1\boldsymbol{C}_2\boldsymbol{C}_3)$ can be recognized by checking which matrix whose elements are all greater than one[2]. Since multiplication of two different matrixes of set (2) is not commutative when $(a+b) \neq 0$, $\boldsymbol{C}_1$ and $\boldsymbol{C}_3$ can be confirmed by checking whether $(\boldsymbol{C}_1^{-1}(\boldsymbol{C}_1\boldsymbol{C}_2\boldsymbol{C}_3)\boldsymbol{C}_3^{-1})$ has the form of the matrixes of set (2). Finally, the corresponding associated matrixes $\boldsymbol{P}_1$ and $\boldsymbol{P}_3$ can be obtained.

Proposition 1. *When $a, b \notin \{0, 1\}$, there is no 1's in the product of any three matrixes (including the same matrixes) of set (2).*

Proof. When $a, b \notin \{0, 1\}$, every element of the four matrixes in set (2) is greater than or equal to one. According to multiplication rule of matrix, it can easily conclude that the proposition held. □

– *Determining $\boldsymbol{P}_0$ and $\boldsymbol{P}_2$ by choosing special $\boldsymbol{L}'_{0,k}$*
If $\boldsymbol{R}'_{0,k}$ is chosen of fixed value zero, it is easy to get

$$\boldsymbol{R}'_{4,k} = \boldsymbol{L}'_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_2) \oplus \boldsymbol{L}'_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1\boldsymbol{P}_2).$$

[2]To simply analysis, the cases when $a, b \in \{0, 1\}$ and elements of multiplication of three matrixes of set (2) are happen to be (1 mod N) are not discussed here.

Construct another special differential image satisfying $\boldsymbol{R}'_{0,k}(i,j) \equiv 0$ and $\boldsymbol{L}'_{0,k}(i,j) = 0$ except that

$$\begin{cases} \boldsymbol{L}'_{0,k}(i_1, j_1) = \alpha_2, \\ \boldsymbol{L}'_{0,k}(i_2, j_2) = \beta_2, \end{cases} \tag{28}$$

where $\gcd(i_1 j_2 - i_2 j_1, N) = 1$ and $\alpha_2 \neq \beta_2$. Then one can use the same method mentioned above to get the permutation matrixes $\boldsymbol{P}_0$ and $\boldsymbol{P}_2$.

- *Step 2) breaking value substitution*:

  From Eq. (7) and Property 3, one can get

$$\boldsymbol{l}_k = \boldsymbol{V}_{5,k} \oplus \boldsymbol{R}_{4,k} \tag{29}$$

and

$$\begin{aligned} \boldsymbol{r}_k &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{L}_{4,k} \\ &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{R}_{3,k} \oplus \boldsymbol{R}_{4,k}(\boldsymbol{P}_3) \\ &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{L}_{2,k} \oplus \boldsymbol{R}_{4,k}(\boldsymbol{P}_3) \\ &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{R}_{1,k} \oplus \boldsymbol{R}_{2,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{4,k}(\boldsymbol{P}_3) \\ &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{L}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{4,k}(\boldsymbol{P}_3) \\ &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{1,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \oplus \boldsymbol{R}_{4,k}(\boldsymbol{P}_3) \\ &= \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{R}_{0,k}(\boldsymbol{P}_1) \\ &\quad \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \oplus \boldsymbol{R}_{4,k}(\boldsymbol{P}_3). \end{aligned}$$

  Substitute $\boldsymbol{R}_{4,k}$ obtained in Eq. (29) into the above equation, one has

$$\begin{aligned} &\boldsymbol{V}_{5,k}(\boldsymbol{P}_3) \oplus \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1) \\ &\qquad = \boldsymbol{l}_k(\boldsymbol{P}_3) \oplus \boldsymbol{r}_k \oplus \boldsymbol{L}_{0,k} \oplus \boldsymbol{R}_{0,k}(\boldsymbol{P}_1) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1). \end{aligned} \tag{30}$$

  Referring to Eq. (23) and Eq. (16), one can get

$$\begin{aligned} \boldsymbol{R}_{4,k} &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{L}_{3,k} \\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{R}_{2,k} \oplus \boldsymbol{R}_{3,k}(\boldsymbol{P}_2) \\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{R}_{3,k}(\boldsymbol{P}_2) \\ &= \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{V}_{2,k}(\boldsymbol{P}_2) \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_2) \\ &\quad \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_2) \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1\boldsymbol{P}_2) \oplus \boldsymbol{R}_0(\boldsymbol{P}_1\boldsymbol{P}_2) \oplus \boldsymbol{V}_0(\boldsymbol{P}_0\boldsymbol{P}_1\boldsymbol{P}_2) \oplus \boldsymbol{L}_0(\boldsymbol{P}_0\boldsymbol{P}_1\boldsymbol{P}_2). \end{aligned}$$

  Hence Eq. (29) become

$$\begin{aligned} &\boldsymbol{V}_{5,k} \oplus \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{V}_{2,k}(\boldsymbol{P}_2) \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_2) \oplus \boldsymbol{V}_{1,k}(\boldsymbol{P}_1\boldsymbol{P}_2) \oplus \boldsymbol{V}_0(\boldsymbol{P}_0\boldsymbol{P}_1\boldsymbol{P}_2) \\ &\qquad = \boldsymbol{l}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_2) \oplus \boldsymbol{R}_0(\boldsymbol{P}_1\boldsymbol{P}_2) \oplus \boldsymbol{L}_0(\boldsymbol{P}_0\boldsymbol{P}_1\boldsymbol{P}_2). \end{aligned} \tag{31}$$

  Substitute $\boldsymbol{L}_{0,k}(\boldsymbol{P}_0\boldsymbol{P}_1)$ obtained in Eq. (30) into Eq. (31) yields

$$\begin{aligned} &\boldsymbol{V}_{5,k}(\boldsymbol{P}_3\boldsymbol{P}_2) \oplus \boldsymbol{V}_{4,k}(\boldsymbol{P}_2) \oplus \boldsymbol{V}_{5,k} \oplus \boldsymbol{V}_{3,k} \oplus \boldsymbol{V}_{1,k} \oplus \boldsymbol{V}_{0,k}(\boldsymbol{P}_0) \\ &\qquad = \boldsymbol{l}_k(\boldsymbol{P}_3\boldsymbol{P}_2) \oplus \boldsymbol{r}_k(\boldsymbol{P}_2) \oplus \boldsymbol{l}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0). \end{aligned} \tag{32}$$

Substitute $\boldsymbol{L}_{0,k}(\boldsymbol{P}_0)$ obtained in Eq. (32) into Eq. (30), one can get

$$\begin{aligned}\boldsymbol{V}_{5,k}(\boldsymbol{P}_3\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{V}_{4,k}(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{V}_{5,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{3,k}(\boldsymbol{P}_1) \oplus \boldsymbol{V}_{5,k}(\boldsymbol{P}_3) \oplus \boldsymbol{V}_{4,k} \oplus \boldsymbol{V}_{2,k} \oplus \boldsymbol{V}_{0,k} \\ = \boldsymbol{l}_k(\boldsymbol{P}_3\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{r}_k(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{l}_k(\boldsymbol{P}_1) \oplus \boldsymbol{l}_k(\boldsymbol{P}_3) \oplus \boldsymbol{r}_k \oplus \boldsymbol{L}_{0,k}. \quad (33)\end{aligned}$$

- *Step 3) decrypting another cipher-image encrypted with the same secret key*:

  Since both Eq. (32) and Eq. (33) exist for any pair of plain-image and its corresponding cipher-image, so one can get

$$\begin{cases} \boldsymbol{L}^{\star}_{0,k} = \boldsymbol{l}^{\star}_k(\boldsymbol{P}_3\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{l}^{\star}_k(\boldsymbol{P}_1) \oplus \boldsymbol{l}^{\star}_k(\boldsymbol{P}_3) \oplus \boldsymbol{r}^{\star}_k(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{r}^{\star}_k \oplus \boldsymbol{M}_{4,k}, \\ \boldsymbol{R}^{\star}_{0,k} = \boldsymbol{l}^{\star}_k(\boldsymbol{P}_3\boldsymbol{P}_2) \oplus \boldsymbol{l}^{\star}_k \oplus \boldsymbol{r}^{\star}_k(\boldsymbol{P}_2) \oplus \boldsymbol{L}^{\star}_{0,k}(\boldsymbol{P}_0) \oplus \boldsymbol{N}_{4,k} \end{cases}$$

  where

$$\begin{cases} \boldsymbol{M}_{4,k} = \boldsymbol{l}_k(\boldsymbol{P}_3\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{r}_k(\boldsymbol{P}_2\boldsymbol{P}_1) \oplus \boldsymbol{l}_k(\boldsymbol{P}_1) \oplus \boldsymbol{l}_k(\boldsymbol{P}_3) \oplus \boldsymbol{r}_k \oplus \boldsymbol{L}_{0,k}, \\ \boldsymbol{N}_{4,k} = \boldsymbol{l}_k(\boldsymbol{P}_3\boldsymbol{P}_2) \oplus \boldsymbol{r}_k(\boldsymbol{P}_2) \oplus \boldsymbol{l}_k \oplus \boldsymbol{R}_{0,k} \oplus \boldsymbol{L}_{0,k}(\boldsymbol{P}_0). \end{cases}$$

  The above equation means that $\{\boldsymbol{M}_{4,k}\}_{k=1}^{n}$, $\{\boldsymbol{N}_{4,k}\}_{k=1}^{n}$, and $\{\boldsymbol{P}_l\}_{l=0}^{3}$ can work together to recover the n least significant bit planes of the right part of $\boldsymbol{l}^{\star}$ and $\boldsymbol{r}^{\star}$, $\{\boldsymbol{L}^{\star}_{0,k}\}_{k=1}^{n}$ and $\{\boldsymbol{R}^{\star}_{0,k}\}_{k=1}^{n}$.

To verify the above analysis, experiments are made with $K_0 = 1234567/(2^{32}-1)$, $T = 4$, and $A = 64$ or 128. First, two special known-images are generated by modifying the image shown in Fig. 3a) to make the differential images satisfy condition (28). Due to similarity of the two constructed plain-image, only one of them is shown in Fig. 6a). Similarly, the other two special known-image are constructed by modifying the image shown in Fig. 3a). The encryption result of the plain-image "Airplane" is shown in Fig. 6b). With the five chosen plain-images, some information about the secret key is obtained to decrypt the cipher-image shown in Fig. 6b) and the result is shown in Fig. 6c). When only A is changed as 128, the recover image of the corresponding cipher-image of the plain-image "Airplane" is shown in Fig. 6d) Once again, the experiment results demonstrate that the breaking performance is mainly by the integer n in Property 2.

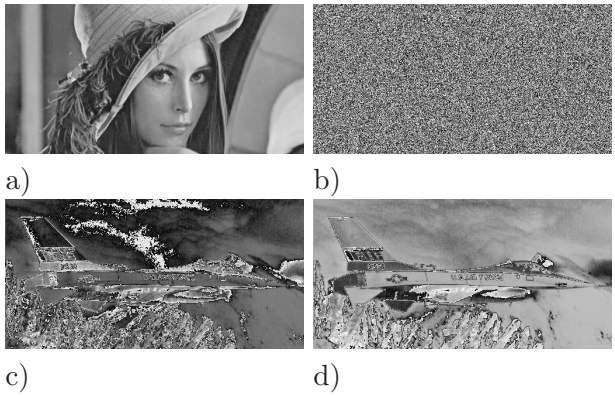

Figure 6: Differential attack on IEAS when $T = 4$: a) chosen plain-image; b) cipher-image of plain-image "Airplane"; c) the recovered plain-image with $A = 64$; d) the recovered plain-image with $A = 128$.

4. Some other security defects of IEAS

To make cryptanalysis on IEAS more complete, some other security defects of IEAS are given in this section.

- The key space of IEAS is not big enough

  In [16, Sec. 4], it is claimed that key space of IEAS is $2^{32(T+2)}$ since PRNS $\{K_l\}_{l=0}^{T+1}$ has $32(T+2)$ bits. However, this it not true since $\{K_l\}_{l=0}^{T+1}$ is generated by the Logistic map under initial condition K_0, who has only n_0 unknown bits, where n_0 is precision length of computer. In fact, permutation matrixes $\{\boldsymbol{P}_l\}_{l=0}^{T-1}$ and mask matrixes $\{\boldsymbol{V}_l\}_{l=0}^{T+1}$ can compose an equivalent secret key of IEAS, and $\{\boldsymbol{P}_l\}_{l=0}^{T-1}$ has only 4^T possible cases. Since generation of $\{\boldsymbol{P}_l\}_{l=0}^{T-1}$ is also controlled by $\{K_l\}_{l=0}^{T+1}$, we can conclude that the real key space of IEAS is only $2^{n_0} \cdot T = 2^{n_0}T$. In [16], $n_0 = 32$, so the key space of IEAS is less than $2^{32}16 = 2^{36}$ considering $T \leq 16$. Even computation precision of 64 bits is used, the key space is only 2^{68}, which is lower than expected size of a secure cipher, 2^{128}, much.

- Insufficient sensitivity with respect to change of plain-image

  As well known in cryptography, sensitivity of ciphertext with respect to changes of plaintext is a very important property measuring a secure encryption scheme. This property is especially important for secure image encryption schemes since a plain-image and its watermarked version are often encrypted in the same time. In [16, Sec. 4.2], it was claimed that IEAS satisfy the property well. However, IEAS fail to do it much due to the following points.

  - The sole nonlinear operation is only used to expand PRBS, and no nonlinear operation, like S-box, is involved of handling plain-image;
  - There is no any operation generating carry bit toward lower level in the whole scheme, so a bit of plain-image can only influence the bits at higher bit planes in the cipher-image;
  - If 2^n $(1 \leq n \leq 7)$ divides variable A in Eq. (5), any change of the bits in the k-th bit plane of plain-image will only affect the bits in the same bit plane of cipher-image for $k = 1 \sim n$.

- Superior performance of IEAS is questionable

  The cryptanalysis presented in the above section is based on the precondition of Property 2, namely 2^n $(1 \leq n \leq 7)$ divides variable A in Eq. (5). This means that IEAS would become robust against the proposed attack if A is odd. Under this condition, Property 2 is still exist with some probability. So, the proposed attack maybe still valid with a little higher complexity. To show inferior performance of IEAS is undoubted in any cases, IEAS is compared with its analogue, DES. The encryption complexity of DES on 128 plain-bits and the widely recognized robustness of DES against differential attack under some rounds are shown in Table 2 [17, 18]. In contrast, encryption complexity of IEAS on the same data and robustness against differential attack are shown in Table 2 also. Although the details deriving attack complexity of IEAS of round number is larger than four are not given here, one can conclude confidently that IEAS is much weaker than DES now.

Table 2: Comparison between IEAS and DES in terms of complexity of encrypting 128 plain-bits and robustness against differential attack, where CP and KP denote chosen plaintexts and known plaintexts, respectively.

Round Number	Complexity		Attack			
	DES	IEAS	Data		Success Rate	
			DES	IEAS	DES	IEAS
1	$O(2^9)$	$O(2^{12})$	$O(1)$CP	2CP	100%	100%
2	$O(2^{10})$	$O(2^{13})$	$O(1)$CP	2CP	100%	100%
3	$O(2^{10})$	$O(2^{13})$	$O(1)$CP	3CP	100%	100%
4	$O(2^{11})$	$O(2^{14})$	2^4CP	5CP	100%	100%
12	$O(2^{12})$	$O(2^{15})$	2^{44}KP	14KP	10%	100%
13	$O(2^{12})$	$O(2^{15})$	2^{45}KP	14KP	10%	100%
16	$O(2^{13})$	$O(2^{16})$	2^{50}KP	14KP	51.3%	100%

5. Conclusion

The security of an image encryption algorithm called IEAS, a block cipher composing of multiple rounds, was studied comprehensively in this paper. Some properties of IEAS are derived to support differential attack on it when its key parameter is even. The detailed approaches for breaking IEAS, when round number is less than five, are presented and can be easily extended to break the version of IEAS of higher rounds. In addition, it is found that encryption results of IEAS is not sensitive with respect to changes of plain-image and its key space is not big enough. Cryptanalysis of IEAS shown in this paper and comparison between IEAS and DES demonstrate IEAS is not attractive secure image encryption scheme and should not be used in applications requiring high level of security.

Acknowledgement

This research was supported by the National Natural Science Foundation of China (No. 61100216), Scientific Research Fund of Hunan Provincial Education Department (Nos. 11B124, 2011FJ2011), and start-up funding of Xiangtan University (Nos. 10QDZ39, 10QDZ40).

References

[1] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos 8 (6) (1998) 1259–1284.

[2] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.

[3] K. Wang, W. Pei, L. Zou, A. Song, Z. Hea, On the security of 3D cat map based symmetric image encryption scheme, Physics Letters A 343 (6) (2005) 432–439.

[4] E. Solak, C. Cokal, O. T. Yildiz, T. Biyikoglu, Cryptanalysis of Fridrich's chaotic image encryption, International Journal of Bifurcation and Chaos 20 (5) (2010) 1405–1413.

[5] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing 91 (4) (2011) 949–954.

[6] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, in: Proceedings of 2002 IEEE International Symposium on Circuits and Systems, Vol. II, 2002, pp. 708–711.

[7] S. Li, X. Zheng, On the security of an image encryption method, in: Proceedings of 2002 IEEE International Conference on Image Processing (ICIP 2002), vol. 2, 2002, pp. 925–928.

[8] S. Li, C. Li, G. Chen, K.-T. Lo, Cryptanalysis of RCES/RSES image encryption scheme, Journal of Systems and Software 81 (7) (2008) 1130–1143.
[9] R. Rhouma, S. Belghith, Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem, Physics Letters A 372 (36) (2008) 5790–5794.
[10] G. Alvarez, S. Li, Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption, Communications in Nonlinear Science And Numerical Simulation 14 (11) (2009) 3743–3749.
[11] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image and Vision Computing 27 (9) (2009) 1371–1381.
[12] C. Li, S. Li, K.-T. Lo, K. Kyamakya, A differential cryptanalysis of Yen-Chen-Wu multimedia cryptography system, Journal of Systems and Software 83 (8) (2010) 1443–1452.
[13] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos 18 (3) (2008) art. no. 033112.
[14] E. Solak, C. Cokal, Algebraic break of image ciphers based on discretized chaotic map lattices, Information Sciences 181 (1) (2011) 227–233.
[15] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.
[16] Y. Zhang, Y. Wang, X. Shen, A chaos-based image encryption algorithm using alternate structure, Science in China Series F-Information Sciences 50 (3) (2007) 334–341.
[17] E. Biham, A. Biryukov, An improvement of Davies' attack on DES, Journal of Cryptology 10 (3) (1997) 195–205.
[18] E. Biham, O. Dunkelman, N. Keller, Enhancing differential-linear cryptanalysis, Lecture Notes in Computer Science 2501 (2002) 587–592.